Mail Security App Wachters

Ruim tweederde van alle e-mails die wereldwijd verzonden worden, zijn ongewenst. De eenvoudigste en hopelijk ook meest effectieve oplossing om e-mails succesvol te filteren, is een e-mail security appliance of kortweg MSA. Data TestLab onderzocht er vijf. JOHAN ZWIEKHORST

Wij kozen vijf MSA's uit die in staat zijn om zeker meerdere tienduizenden zoniet honderdduizenden berichten per dag te screenen. Mocht uw bedrijf dagelijks slechts een paar honderd of een paar duizend e-mails binnenkrijgen, dan kunt u wel nog toekomen met wat extra beveiligingssoftware op uw mailserver. Zijn het er meer, dan wordt een appliance zoals hier besproken een noodzakelijke investering.

Bij de appliances was het onze doelstelling dat er voor u als onderneming zo weinig mogelijk beheer aan moet zijn. Inpluggen en werken verdient de voorkeur. We moeten natuurlijk wel wat rapporten kunnen opvragen zodat we weten wat er gebeurt en we moeten ook een behoorlijke quarantaine-oplossing hebben voor de twijfelgevallen bij de mails die we binnenkrijgen. We hebben het gehouden bij MSA's van BorderWare, CipherTrust, IronPort, SonicWall en Sophos. We hebben ze elk ongeveer minstens een week tot tien dagen lang in een live omgeving gehangen. Onze testprocedure bestond erin dat we een zo standaard mogelijke configuratie gebruiken en nagaan hoeveel ongewenste mails nog in onze mailboxen terecht komen, maar ook of er legitieme mails zijn die toch geblokkeerd raken (valse positieven).

BorderWare MXtreme Mail Firewall

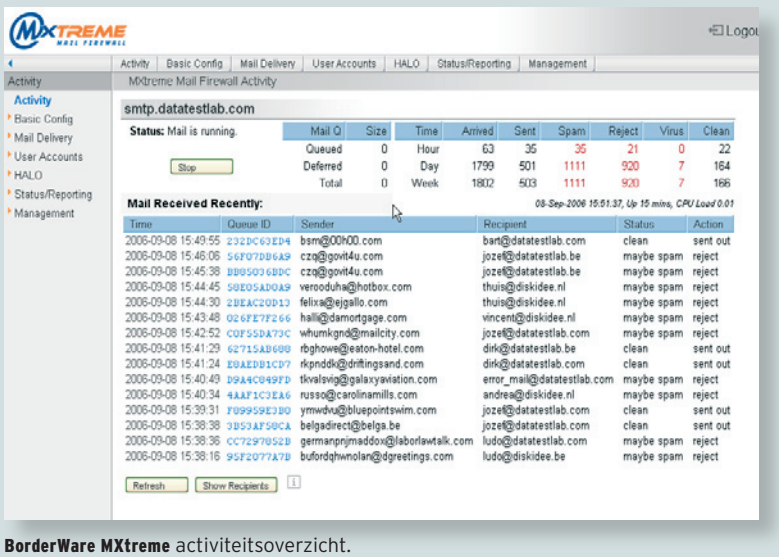
De appliance die BorderWare voor de test inleverde, is een één rekeenheid hoge pizzadoos met drie netwerkpoorten en twee harde schijven in een RAID-1 configuratie. Vooraan is er een lcd-paneel met een ingebouwd menusysteem. Een eigenaardigheid is dat BorderWare niets voorzien heeft om de initiële installatie van de appliance via het netwerk uit te voeren: u moet een scherm en toetsenbord (muis is optioneel) aansluiten om die installatie uit te voeren.

Beheer

BorderWare heeft zijn webinterface erg eenvoudig gehouden. Behalve uw webbrowser hebt u niets anders nodig. De beheerinterface vertrekt vanuit een eenvoudig menusysteem. De zeven hoofdfuncties zijn: Activiteit, Basisconfiguratie, Postbedeling, Gebruikersprofielen, HALO, Status/Rapportage en Beheer. De keuze 'Activiteit' brengt u naar het hoofdscherm en toont een overzicht van alle activiteiten van de postverwerking. In het hoofdmenu-item 'Gebruikersprofielen' kunt u gebruikers en gebruikersgroepen definiëren of synchroniseren met een LDAP- of Active Directory-server. Onder 'Mail Delivery' (postbedeling) valt alles wat er moet gebeuren met binnenkomende of uitgaande e-mails. 'Status/Rapportage' omvat alle logs, statistiek- en rapportgeneraties maar ook de quarantaines voor mails met virussen, spam of andere ongewenste inhoud. Onder 'Beheer' zien we systeemfuncties die met het beheer van de appliance zelf te maken hebben: back-up en restore, updates en patches, licentiebeheer, maar ook het uitschakelen of herstarten van de appliance. De menuoptie HALO omvat clustering, replicatie en integratie met F5 iControl. Als u meerdere appliances in gebruik hebt, kunt u die overigens centraal beheren vanuit één webinterface.

Beveiliging

Hoewel het mogelijk is om aparte beveiligingsreglementen op te stellen voor elke netwerkpoort, omvatten de standaardvoorzieningen van een beveiligingsreglement zowel controles voor inkomende als uitgaande post.



BorderWare MXtreme activiteitsoverzicht.

liances

tegen ongewenste e-mail

Die controles omvatten een viruswering met behulp van Kaspersky, antispam, controle van het soort bijlage en meer diepgaande inhoudsfiltering. Voor de spamblokkering is Intercept voorzien, dat is BorderWare's eigen spamfilter. Als u dat wenst, kunt u een licentie voor BrightMail van Symantec aanschaffen en dan wordt die spamfilja, kan zijn toegang voor het afleveren van mail gestaakt worden of onderworpen aan strikte beperkingen.

Prestaties

In onze test kregen we nog ruim een gemiddelde van 24 foute berichten per dag en per mailbox binnen en we stelden van drie legitieme berichten

De vijf geselecteerde MSA's zijn in staat om vele tienduizenden tot honderdduizenden berichten per dag te screenen

ter nog eens extra in gebruik genomen. BorderWare maakt zich echter sterk dat Intercept voldoende krachtig is opdat u ook zonder BrightMail kunt. Intercept bevat allerlei faciliteiten die het ontdekken van spam moeten verbeteren: spambibliotheken, IP-reputatie en domeinsleutels.

BorderWare heeft ook het BorderWare Security Network of kortweg BSN opgericht waarmee informatie uitgewisseld kan worden over zenders van e-mail: hun reputatie, of het om een inbeller gaat, of hij grote hoeveelheden post verzendt en hoeveel daarvan reeds besmet bleek met een virus of spam was. Spambibliotheken zijn eigenlijk niet nieuw: het gaat om woordenlijsten met woorden die vaak in spamberichten opduiken. Deze spambibliotheken moeten ervoor zorgen dat spamfilters niet of veel minder getraind moeten worden vooraleer ze effectief spam kunnen bestrijden.

Domeinsleutels zijn een populaire manier om mailzenders te valideren. Daarnaast kan MXtreme 6 gebruik maken van dreigingspreventie. Met deze preventie kunnen maildoorstromingspatronen onderzocht en geëvalueerd worden en zo kan de appliance beoordelen of een zender zich schuldig maakt aan kwaadaardig gedrag. Indien vast dat ze geblokkeerd werden. Dat zou heel wat beter moeten.

Productinfo
Product: MXtreme Mail Firewall
Producent: BorderWare; www.borderware.com
Leverancier: NOXS Netherlands, tel. 030-6025400; www.nl.noxs.com
Adviesprijs: 17.860 euro (MX400 Email Security Bundle incl. 12 maanden onderhoud en garantie)

CipherTrust IronMail

CipherTrust heeft een e-mailbeveiligingsappliance met de naam IronMail geproduceerd en het zal wel geen toeval zijn dat die naam erg doet denken aan de elders besproken IronPort. De IronMail appliance die we binnenkregen voor onze test is het basismodel en behoort tot de zogenaamde S-klasse. Dat is een één rekeenheid hoog toestel dat onder FreeBSD draait en één enkele netwerkpoort heeft. CipherTrust heeft daarboven nog een E-klasse en de topmodellen behoren tot de C-klasse. Al die appliances werken met dezelfde IronMail-software. CipherTrust gebruikt een dubbele antivirusengine: van McAfee en van Authentium.

Beheer

Het webbeheer ziet er leuk uit en elk gekozen hoofdrubriek toont een stel overzichtsgrafiekjes en -rapporten. De tien hoofdrubrieken zijn: Dashboard, Queue Manager (wachtrijbeheerder), Compliance (reglementnaleving), Anti-Spam, Anti-Virus, Encryption (encryptie), Intrusion Defender (inbraakverdediging), Reporting (rapportage), Administration (appliancesoftware- en webbeheer) en System (systeembeheer). De wachtrijbeheerder geeft u controle over heel wat wachtrijen, want er kan een wachtrij aangemaakt worden voor bijna elke beveiligingsregel. Zo zijn er aparte quarantainewachtrijen voor spam vanaf 50 punten, spam vanaf 75 punten en spam van 100 punten. Naar onze ervaring kunt u spam van 100 punten gewoon laten schrappen, daar hebben we gedurende de testperiode geen enkele valse positieve in gevonden. Voor spam vanaf 50 en 75 punten kunnen we dat echter niet zeggen.

'Compliance' gaat onder meer over inhoudsfiltering, maar ook over analyse van de berichthoofding, adresseringen, bijlagen, eventuele encrypties en een witte lijst. Maar ook onder antispam en antivirus kunt u heel wat opties instellen. CipherTrust maakt gebruik van een reputatiefiltersysteem dat TrustedSource heet, maar het is veel minder uitgebreid en wijdverspreid dan het SenderBase-systeem van IronPort. Er zijn meer instellingen mogelijk dan nodig of wenselijk is voor MKB's, maar het goede nieuws is dat u ze niet hoeft op te roepen als de standaardinstellingen voor u voldoen.

De inbraakverdediging heeft te maken met pogingen om in te breken op de appliance of om de postverwerkende diensten plat te leggen. De rap-

portagerubriek bevat een heel gamma aan voorgedefinieerde rapporten in PDF- en HTML-formaat. U kunt zelf nieuwe rapporten bijmaken, maar in essentie gaat dat over het vergaren van gegevens uit de logbestanden en die dan in csv-formaat presenteren. Rapporten kunnen ook geautomatiseerd gegenereerd worden en dan geëmaild of via ftp op een server bewaard worden.

Prestaties

Voor de goede werking van TrustedSource maakt de CipherTrust appliance gebruik van een paar uitbreidingen in de dns-standaard. Helaas blijken die uitbreidingen niet ondersteund te worden door de dns-servers van Microsoft Windows en van verschillende Unix-systemen van providers. In zo'n geval werkt TrustedSource gewoon niet en dan laat de appliance veel te veel spam door: in ons geval daalde dat tot slechts 6 à 7 spamberichten per mailbox en per dag. Nu blijkt dat weinig courant gebruikte dns-servers de door CipherTrust vereiste dns-uitbreidingen ondersteunen, heeft CipherTrust aangekondigd een dns-serverfarm te zullen oprichten speciaal voor hun mailfilterappliances zodat TrustedSource keurig zal werken. Helaas moesten we ook vaststellen dat over de duur van de testperiode maar liefst 23 legitieme berichten uit de spamquarantaine gered moesten worden. Dat is helaas het hoogste aantal van alle geteste appliances. CipherTrust heeft dus duidelijk nog flink wat werk aan hun spamfilter.

Productinfo

Product: IronMail
Producent: CipherTrust; www.ciphertrust.com
Leverancier: SecureComm, tel. 010-5191466, www.securecomm.nl
Adviesprijs: 6.195 euro (appliance plus 250 licenties), minimumlicentie is 3.895 euro voor 50 licenties

konden we onze eigen dns-servers en ook die van onze provider Verizon niet gebruiken en kwamen we aan zo'n 50 spamberichten die nog doorgelaten werden per mailbox en per dag.

Nadat we de dns-servers van CipherTrust zelf ingevuld hadden, een C300/C600 voor tussen 1.000 en 10.000 gebruikers en het topmodel is de X1000 die bedoeld is voor ISP's en tot één miljoen berichten per uur aan kan.

Beheer

U beheert de IronPort appliance via een rechtlijnige webinterface. Er zijn vijf tabbladen: Monitor (bewaking), Mail Policies (postreglementen), Security Services (beveiligingsdiensten), Network (netwerkinstellingen) en System Administration (systeembeheer). Onder 'Monitor' (bewaking) bekijkt u alleen statusinformatie en vraagt u allerlei statistieken en rapporten op. Bij 'Mail Policies' stelt u uw beveiligingsreglementen op. U kunt reglementen en inhoudsfilters definiëren voor inkomende en buitengaande post. Die inhoudsfilters kunt u trouwens opgeven binnen een mailreglement, want daarin legt u vast

Spambibliotheken moeten ervoor zorgen dat spamfilters niet of veel minder getraind moeten worden vooraleer ze effectief spam kunnen bestrijden

IronPort C100

IronPort heeft verschillende modellen appliances afhankelijk van het volume aan post dat u wilt verwerken. De C100 die we hier bespreken is het kleinste model en kan tot duizend gebruikers (mailbestemmelingen) aan. Er is nog wat er onder welke voorwaarden moet gebeuren met post in verband met antispam, antivirus, inhoudsbeheer en virusuitbraakfilters (die bespreken we in de volgende paragraaf). De spamfilter is trouwens van eigen makelij en de antivirusmotor is van Sophos. Desgewenst kunt u ook kiezen voor een Symantec BrightMail spamfilterengine, maar volgens IronPort is dat nergens voor nodig en presteert hun eigen spamengine minstens zo goed terwijl de licentie goedkoper is. Er zijn erg veel mogelijkheden en dat kan overdonderend werken, maar IronPort heeft rekening gehouden met beheerders die nog niet eerder met IronPort gewerkt hebben en dus vertrekt de appliance met een gemakkelijk te volgen vijfstappenwizard die enkel de hoogstnodige vragen stelt en dan standaardreglementen invoegt en toepast.

Het tabblad 'Security Services' toont een overzicht van alle beveiligingsdiensten en u krijgt van elke dienst een statusoverzicht en de mogelijkheid om meteen de laatste nieuwe updates af te halen (dat kan natuurlijk ook volautomatisch). De diensten zijn: antispam,

CipherTrust IronMail statusoverzicht.

antivirus, virusuitbraakfilters, SenderBase-participatie (virusuitbraakfiltering en SenderBase bespreken we in de volgende paragraaf) en dienstenupdates. Het voorlaatste tabblad, 'Network', omvat alle netwerkspecifieke instellingen zoals de IP-adressen van elke interface en u kunt meerdere aliassen definiëren: in feite ondersteunt IronPort tot 256 IP-adressen

Beveiliging

Eén van de redenen waarom meer traditionele mailfilters erg vertragend werken, is dat zij de beveiliging erg serieel aanpakken. Zo haalt een traditionele mailfilter eerst een bericht volledig binnen, daarna gaat het door een spamfilter, dan door een virusfilter en wat dan nog overblijft wordt onderworpen aan het bedrijfsbeveiligingsreglement. Dan pas komt de mailrouting aan de beurt en kan het afgeleverd worden aan de groupwaresoftware. U begrijpt al dat dit seriële afhandelingsproces de boel behoorlijk kan vertragen en dus het aantal e-mailberichten dat zo'n oplossing kan verwerken sterk beperkt.

Bijna alle andere spamfilters op de markt proberen eerst aan de hand van de berichthoofding zoveel mogelijk berichten te elimineren, maar normaal doen ze dat met zwartelijstservers op het internet. Zwartelijstservers zijn servers die een raadpleegbare zwarte lijst bijhouden van mailservers die ooit spam verzonden hebben. Het probleem is, dat een mailserver vrij vlug op zo'n zwarte lijst terecht kan komen en dat het verdomd moeilijk is weer uit de lijst verwijderd te worden. Daarom werkt IronPort met een zogenaamde reputatiescore. Daartoe gebruikt IronPort een wereldwijd informatievergaringssysteem dat SenderBase heet. De bedoeling is dat alle IronPort-mailfilters informatie vergaren over wie post verzendt via hun systemen en of die zender te goeder trouw is dan wel virussen of spam zendt of eventueel tot dusver onbekend is. Op basis van meer dan 110 parameters voor mail en 50 parameters voor websites en weblinks krijgt iedere mailserver in de lijst een reputatiescore toegewezen. Bij iedere nieuwe mailtransmissie wordt die score verder automatisch bijgewerkt. Een reputatiescore kan lopen van -10 (heel slecht) over 0 (onbekende mailserver) naar +10 (heel erg goed). Een zwarte lijst op internet werkt binair: ofwel sta je op de zwarte lijst, ofwel niet. Meer keuze is er niet. Met SenderBase kan elke mailserver twintig verschillende waarden toegewezen krijgen en op die manier is de beoordeling niet meer zwart/wit, maar met heel wat grijs ertussen.

Overigens verzamelt het SenderBase systeem nog meer gegevens. Zo kan het systeem opmerken dat bepaalde soorten bijlagen bij e-mails ineens meer dan normaal voorkomen en op die manier de verspreiding van nieuwe virussen via

e-mail detecteren en blokkeren nog voordat de antivirusproducenten hun signatuurbestanden hebben aangepast en gedistribueerd. Een van de beveiligingssystemen bij IronPort is dan ook de virusuitbraakfilter. Dat is een filter die werkt met regels voor soorten bijlagen en het mogelijk schadelijke effect daarvan. U kunt overigens kiezen of de mails die uw IronPort-systeem verwerkt gebruikt mogen worden op het SenderBase-systeem te updaten of niet. Wij zien in elk geval geen reden om niet mee te werken aan SenderBase.

Prestaties

IronPort C100 is wat ons betreft een bijzonder interessante mailbeveiligingsappliance. Het werken met mailstatistieken die leiden tot het gebruik van een reputatiescore in plaats van een gewone zwarte lijst en virusuitbraakdetecties zijn stevige pluspunten. Tijdens onze testperiode kwamen gemiddeld tussen drie en vier ongewenste mails per dag en per mailbox door en dat is meteen de beste score van alle hier geteste appliances. Er werden geen legitieme mails geblokkeerd. Een aanrader!

Productinfo

Product: IronPort C100
Producent: IronPort; www.ironport.com
Leverancier: IronPort Systems Benelux, tel. +32 476 59 36 60; www.ironport.com
Adviesprijs: 4.200 euro (C100 MTA, Content Scanning, Reputation Filtering, Licentie IronPort Antispam 100 users, Licentie Virus Outbreak Filters 100 users, Licentie Sophos Antivirus 100 users, Licentie Mail Flow Central)
Standaard in alle bundles: MTA, Reputation Filtering, Content Management, Mail Flow Central (Reporting & Tracking), Platinum Support.
Verschillende versies: Enkel IronPort AS, IronPort AS + Sophos AV, IronPort AS + Sophos AV + Virus Outbreak Filters
Tevens bundles verkrijgbaar met redundant units.

SonicWall ES500

De SonicWall appliance die we hier bekijken heet voluit 'Email Security 500' of korter ES500. Het gaat om een 19-inch rekappliance van één rekeenheid hoogte en die niet al te diep is. Er zijn aansluitingen voor VGA, toetsenbord en muis maar die hebt u niet nodig. Gewoon de netwerkaansluiting in uw netwerk pluggen en u bent vertrokken.

De C100 appliance van IronPort haalt de allerbeste prestaties met gemiddeld minder dan vier spamberichten per dag en per mailbox

Alle SonicWall ES-appliances hebben dezelfde functionaliteit aan boord, de verschillende modellen verschillen naargelang hun verwerkingscapaciteit: ES200, ES300, ES400 en ES500. Deze modellen zijn allemaal bedoeld voor MKB's. SonicWall heeft ook nog een enterprise-serie met nog meer capaciteit en dat zijn dan de modellen ES6000 en ES8000. SonicWall deelt zijn appliances in volgens het aantal gebruikers (of mailboxen) dat u wil gaan ondersteunen. De modellen zijn dus bedoeld voor maximum 50, 100, 250, 1000, 5000 en voor meer dan 5000 gebruikers, respectievelijk.

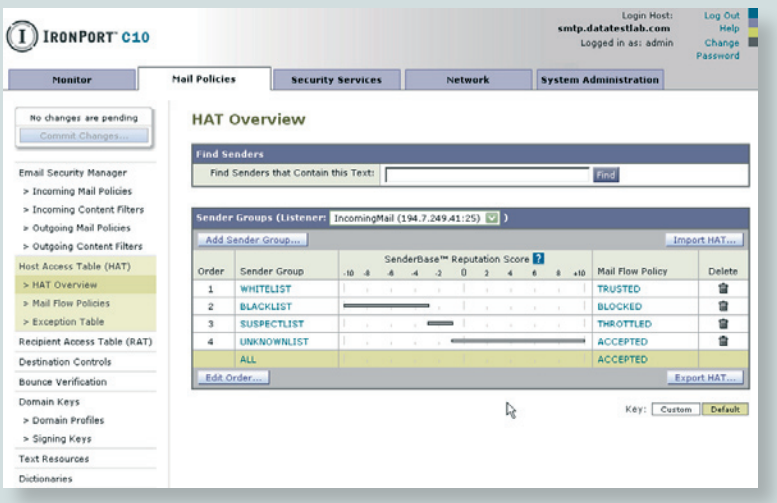
De SonicWall appliances draaien onder het SonicOS besturingssysteem, een door SonicWall speciaal aangepaste versie van Linux. Daarbovenop draait een e-mail security applicatie en die heet SonicWall Email Security en heeft momenteel versie 4.7, met versie 5.0 op komst. Overigens bestaat deze sofware ook in een versie voor Windows 2000 of 2003 servers en die kunt u dan zelf draaien.

Installatie en configuratie

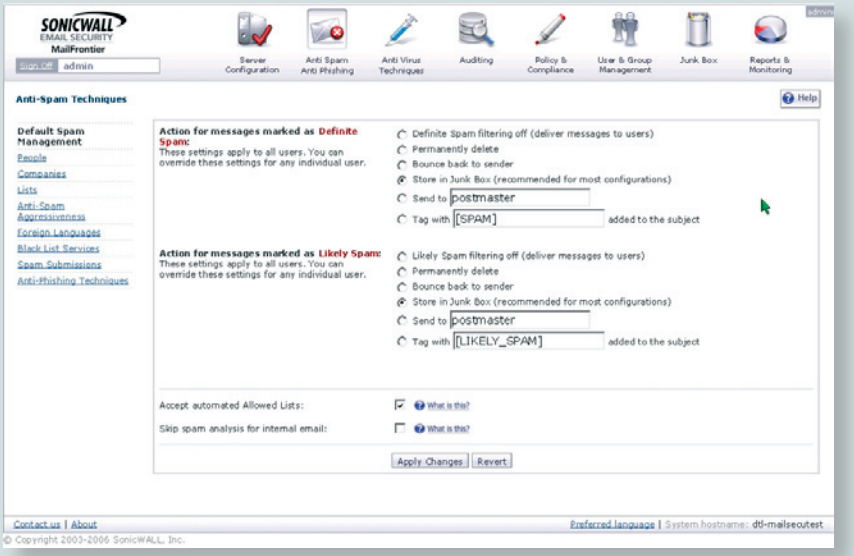
U doet normaal het hele beheer van de SonicWall appliance via zijn webinterface. Let wel: de SonicWall appliances werken met jaarlijks te vernieuwen licenties en daartoe moet u als klant geregistreerd zijn op de website van SonicWall en moeten al uw SonicWall-producten ook geregistreerd zijn, samen met hun licenties. Alleen als dat het geval is, kan zo'n appliance behoorlijk geconfigureerd worden en werken

Beheer

Nadat uw appliance geconfigureerd is en voorzien van alle benodigde licenties, krijgt u standaard een rapportagedashboard te zien met grafiekjes van alle verwerkte in- en uitgaande post die u in één oogopslag laten zien hoeveel u geteisterd wordt door ongewenste mails en wie daar in uw bedrijf de grootste slachtoffers van zijn. De appliance kan met succes gebruikt worden door de beveiligingsmodules waarvoor u een licentie hebt in te schakelen. U kunt de beveiliging verder verfijnen door een e-mailbeveiligingsreglement op te stellen (zoniet gebruikt de appliance de standaardregels van SonicWall) en eventueel de appliance gebruik te laten maken van blacklistservers op internet. SonicWall laat u trouwens desgewenst twee antivirusengines toepassen: McAfee en Kaspersky. U kunt één van hen kiezen, maar ook beide. Misschien vindt u dat zinloos, maar naar onze ervaring vindt één antiviruspakket nooit alle virussen. Door twee virusscanners na elkaar te draaien, vermindert u het risico dat er toch nog een virus door-



IronPort postaflevertoegangsreglement.



SonicWall antispamconfiguratie.

raakt. Natuurlijk hangt daar voor die extra veiligheid qua licenties wel een prijskaartje aan vast.

Prestaties

Wij hebben de appliance in de live omgeving gezet zonder extra beveiligingsreglement buiten de spamfilter en met de twee antivirusengines actief. Dat leverde gemiddeld nog altijd zo'n 60 ongewenste mails op per dag en per mailbox en dat is dus veel te veel. Zoals eerder aangehaald zou dit wel verbeterd kunnen worden door bijkomende beveiligingsregels te definiëren en gebruik te maken van externe blacklistservers, maar dat hebben wij dus net als bij de andere geteste appliances niet gedaan. In de testperiode werden een vijftal berichten onterecht geblokkeerd. Ook dat is veel te veel en zou beperkt kunnen worden met een paar goed gekozen bijkomende regels.

Productinfo

Product: E-mail Security 500
Producent: SonicWall; www.sonicwall.com/products/emailsecurity/productline.html
Leverancier: ACAL Nederland (www.acal.nl), Azlan Nederland (www.azlan.nl), E92Plus (www.e92plus.nl)
Adviesprijs: 7.771,14 euro (ES500 appliance tot 2000 gebruikers); 2.511 euro (jaarlijks e-mailbeschermingsabonnement plus 8x5 dynamic support voor tot 2000 gebruikers en één server).

Sophos ES4000

Ook het Britse bedrijf Sophos wil diversifiëren: van antivirusproducent naar beveiligingsspecialist. Vandaar de introductie van onder meer een eigen spamfilter, die u nu ook in een complete appliance kunt krijgen. De ES4000 e-mailbeveiligingsappliance controleert e-mails op virussen, spam en ongewenst taalgebruik. Het systeem werkt onder FreeBSD met een Postfix MTA. De ES4000 is een appliance van één rekeenheid hoog.

Beheer

Sophos heeft het beheer zo eenvoudig mogelijk gehouden. Bovenaan krijgt u een knoppenbalk met vijf hoofdrubrieken: Dashboard, Configuration, Reports, Search, Help en Status. Die laatste ziet er iets anders uit en wellicht merken veel beheerders daarom niet eens op, dat dit wel degelijk een aanklikbare rubriekfunctie is. Ze toont een overzicht van de systeemstatusinformatie met zonodig aanklikbare pop-ups met systeemwaarschuwingen. Dashboard is zoals bij veel andere systemen een overzicht van de postverwerking inzake capaciteit versus belasting, spam versus ham en uiteraard de virusinfecties. Het ziet er leuk uit en geeft een goed overzicht van de postverwerkingsstatus. Het is ook het eerste scherm dat een beheerder te zien krijgt na de inlog. De rubriek Configuratie toont links een boomstructuur van aanklikbare tekstlinks en rechts daarvan de detailinformatie die bij de gekozen link hoort. De tekstlinks uiterst links zijn onderverdeeld in zes kleine rubriekjes: Accounts (beheerder- en gebruikersinstellingen), Policy (instellingen voor antivirus, antispam, inhoudsfilters, witte en zwarte lijsten), Systeem (updates, waarschuwingen, back-up, Active Directory-integratie, en tijdzone-instellingen), Routing (mailservers, maildomeinen en relays) plus Netwerk (netwerkinterfaces, domeinnaam en proxy, netwerkconnectiviteit). Bij de Policy-rubriek is er over het algemeen weinig in te stellen inzake de eigenlijke detectie van ongewenstheden, maar wel wat er moet gebeuren met mails die een bepaalde score bereikt hebben. Veel meer dan kiezen wat er moet gebeuren met mails met een hoge of middelmatige score behelst dat echter niet, al kunt u wel regels definiëren voor bepaalde bestemmingen en daar uitzonderingen op maken.

De hoofdrubriek Reports geeft een aantal voorgedefinieerde rapporten. U kunt ze verfijnen met zoekparameters, maar zelf nieuwe rapporten definiëren is niet echt mogelijk. De hoofdrubriek Search (Zoeken) geeft inzage in de postverwerkingslogs, de quarantaine en de postwachtrijen. U gebruikt deze functie om na te kijken wat er met uw post gebeurt en om de postquarantaine te inspecteren en er eventueel berichten uit te redden.

Het webbeheer ziet er leuk uit en elk gekozen hoofdrubriek toont een stel overzichtsgrafiekjes en -rapporten

Prestaties

Tijdens onze testperiode liet de ES4000 gemiddeld zo'n 17 spamberichten per dag en per mailbox door en we moesten zes legitieme berichten redden. Die valse positieven zaten wel allemaal in de 'medium spamscore'-categorie, alles van 'high spamscore' bleek effectief en zonder uitzondering spam te zijn. We raden u dus aan bij deze appliance alleen

spamberichten met een hoge score te verwijderen en al het andere voor de veiligheid in quarantaine te plaatsen. Die moet u dan natuurlijk wel regelmatig uitwieden om de legitieme berichten (waarvan u dus niet op voorhand weet of die erin zitten of niet) te kunnen redden. Al bij al heeft ook Sophos dus nog wat werk aan hun spamfilter: het aantal valse positieven is bijvoorbeeld nog te hoog.

Productinfo

Product: ES4000 Email Security Appliance
Producent: Sophos; www.sophos.com
Leverancier: Sophos Benelux, 0183-641064; www.sophosbenelux.com
Adviesprijs: 16.200 euro (waarvan 9.200 euro voor de hardware + 7.000 euro voor de software met een licentie van 1 jaar)

Conclusie

Uit deze test blijkt overduidelijk de superioriteit van IronPort met zijn C100 appliance. Ze haalt de allerbeste prestaties met gemiddeld minder dan vier spamberichten per dag en per mailbox en we moesten geen enkel legitiem bericht redden. Ze heeft bovendien nog een erg redelijke prijs ook en is de echte aanrader van deze test. Op de tweede plaats komt voor ons de CipherTrust IronMail appliance, die ook een erg redelijke prijs heeft met een uitstekende spamfiltering op voorwaarde dat de TrustedSource reputatiefiltering vlekkeloos werkt, maar als grote nadeel een te grote hoeveelheid valse positieven laat zien. Vrijwel alles in quarantaine laten staan en dat dagelijks uitwieden is dus de boodschap. De appliances van BorderWare en Sophos zijn het duurst en laten nog een tiental spamberichten per dag en per mailbox door met gemiddeld één vals positief bericht om de twee dagen: die komen bij ons op de derde en vierde plaats terecht. SonicWall heeft wel een interessante prijs en doet het lang niet slecht met gemiddeld één vals positief bericht om de twee dagen, maar laat met gemiddeld 60 spamberichten per dag en per mailbox teveel rommel door om geen ergernis te veroorzaken bij de gebruikers. Daarom eindigt hij in deze test laatst, al heeft hij wel de meest gunstige prijs.

Sophos rapportage.